ULTRALIFE

WAVEFORM IDENTITY

Your body is your credential.
Your heartbeat is your signature.
Your waveform is your DNA.

Technical Specification v1.0
February 2026 · Confidential

UltraLife Protocol · Resonance Systems · Mechanical Battery LLC

Contents

1. The Eigenvector Identity

> *In linear algebra, an eigenvector is a vector that maintains its direction under transformation.*
>
> *Only its magnitude changes, scaled by the eigenvalue λ.*
>
> *Your biometric waveform is an eigenvector: the pattern that persists regardless of what*
>
> *transformations are applied — different day, different mood, different environment.*
>
> *The eigenvalue is the confidence score.*

Every identity system in history has been based on something you have (a key, a card), something you know (a password, a PIN), or something you are (a fingerprint, a face). The first two can be lost, stolen, or forgotten. The third can be photographed, lifted, or faked from static samples.

Waveform identity introduces a fourth category: something you ARE, continuously, in real time. Not a static snapshot of your fingerprint. Not a photograph of your face. A living, time-varying, multi-dimensional signal that is generated by your body every moment you exist. It cannot be stolen from a database because it is not static. It cannot be replicated from a recording because biological liveness — beat-to-beat cardiac variability, respiratory sinus arrhythmia, circadian drift — makes every moment's signature unique while maintaining the persistent eigenvector direction that identifies you.

This document specifies how UltraLife implements waveform identity as its core authentication layer, how it maps to the Cardano blockchain, how it converges with genetic identity over time, and how it handles the hardest adversarial case: someone actively trying to spoof or block their waveform.

2. Mathematical Foundation

2.1 The Identity Eigenvector

Let W(t) be your body’s spectral signature at time t — a high-dimensional vector in waveform space. W(t) varies with time (your heart rate changes, you move, you sleep, you exercise), but it varies around a stable attractor.

Define the identity function I as the time-averaged spectral feature vector:

> $I = \langle \Phi(W(t)) \rangle_t$ *where Φ is the feature extraction function and $\langle \cdot \rangle$ denotes time averaging*

I is your eigenvector. Under daily transformations T (sleep, exercise, stress, meals), your waveform changes but your identity vector persists:

> $T \cdot W(t) = \lambda(t) \cdot W(t) + \varepsilon(t)$ *where $\lambda(t)$ is the eigenvalue (confidence) and $\varepsilon(t)$ is noise*

Authentication succeeds when the cosine similarity between a live reading and the enrolled identity exceeds a threshold:

> $auth(W\_live) = true$ *iff* $\cos(I\_enrolled, \Phi(W\_live)) > \theta$ *where θ is typically 0.85–0.95*

2.2 Multi-Modal Feature Space

A single biometric modality (cardiac alone, gait alone) has limited discriminative power. The identity vector combines multiple modalities into a joint feature space:

Modality	Dimension	Uniqueness Contribution	Spoofability
Cardiac morphology (PPG waveform shape)	~40 features	High — ion channel genetics	Medium — requires cardiac model
Heart rate variability (HRV spectral)	~20 features	High — autonomic signature	Hard — requires real-time ANS model
Gait / micro-movement (accelerometer)	~30 features	Medium — musculoskeletal	Medium — gait is observable
Touch dynamics (screen interaction)	~25	Medium — neuromuscular	Hard — subconscious

	features		patterns
Voice spectral (vocal tract resonance)	~35 features	High — anatomical geometry	Medium — voice synthesis exists
Impedance spectroscopy (crystal phase)	~50 features	Very high — tissue composition	Very hard — requires body model

Combined feature vector: ~200 dimensions (phone phase) scaling to ~400+ dimensions (crystal phase). The joint space is exponentially harder to spoof than any single modality because the attacker must maintain cross-modal consistency.

2.3 Uniqueness Estimation

With N independent features each having k distinguishable levels, the identity space has k^N possible states. Conservative estimate: 200 features with 10 distinguishable levels per feature = 10^{200} possible identities. This exceeds DNA STR profiling (~$10^{1.6}$ with 20 loci) by over 190 orders of magnitude.

In practice, features are not independent and some levels are more common. Realistic uniqueness estimation requires population-level data from EXP-004 style studies. But the dimensional advantage over DNA profiling is structural, not marginal.

3. Sensor Architecture

3.1 Phone Phase (Now — No Hardware Required)

Sensor	Signal	Method	Quality
Rear camera + flash	Cardiac PPG waveform	Finger on camera, red channel captures blood volume pulse	Clinical-grade HR/HRV. Waveform morphology usable.
Accelerometer	Gait + micro-movement	Continuous background, phone in pocket or hand	Good for gait. Excellent for device-in-hand dynamics.
Gyroscope	Rotational movement	Complements accelerometer for 6-DOF movement	Adds orientation to movement signature
Touch screen	Pressure + timing + swipe	Passive during normal phone use	Behavioral biometric. Very hard to consciously replicate.
Microphone	Vocal spectral	Short enrollment phrase + ambient voice capture	Good for tract geometry. Sensitive to environment noise.
Barometer (if present)	Respiratory rate	Micro-pressure changes from breathing near phone	Supplementary. Low resolution.

Phone phase captures 4–5 modalities simultaneously. Enrollment takes 60 seconds. Continuous authentication runs passively using accelerometer + touch dynamics with periodic PPG re-verification.

3.2 Crystal Phase (Resonance Device)

Sensor	Signal	Advantage Over Phone
Piezoelectric crystal (chest-coupled)	Cardiac mechanical waveform (BCG/SCG)	Direct body contact. Higher SNR. Full waveform morphology.
Fractal filterbank (27-band)	Multi-band spectral decomposition	Analog decomposition at biological frequencies. No ADC aliasing.
Impedance spectroscopy drive	Tissue composition through body	Reads genetic expression of tissue properties. Phone cannot do this.
Thermal harvester (also sensor)	Skin temperature + thermal flux	Continuous thermal signature. Phone has no skin contact.
Haptic transducer (also sensor)	Micro-vibration coupling	Bidirectional: senses and communicates simultaneously.
Mesh coupling (inter-	Proximity + coupling	Two crystals detect each other’s carriers. Phone

device)	dynamics	Bluetooth cannot.

Crystal phase adds impedance spectroscopy and direct body coupling, which are the modalities that converge with genetic identity. The phone phase establishes the identity system; the crystal phase deepens it.

4. Feature Extraction Pipeline

4.1 Cardiac Features (PPG / Piezo)

From raw PPG or piezo cardiac waveform, extract per-beat and statistical features:

Feature Class	Examples	Count
Morphological	Systolic peak amplitude, diastolic notch depth, pulse width at 50%, rise time, T-wave shape	~15
Interval	RR interval, QT proxy, pre-ejection period, pulse transit time (if two sensors)	~8
Variability	SDNN, RMSSD, pNN50, HRV power (VLF, LF, HF bands), LF/HF ratio, sample entropy	~12
Spectral	Dominant cardiac frequency, harmonic structure (2nd–5th harmonic ratios), spectral centroid	~8

Total cardiac features: ~43. The morphological features are the most genetically determined (ion channel kinetics). The variability features are the most liveness-sensitive (impossible to fake without real-time ANS modeling).

4.2 Movement Features (Accelerometer + Gyroscope)

Feature Class	Examples	Count
Gait cycle	Step frequency, stride symmetry, heel-strike acceleration, stance/swing ratio	~12
Postural	Static sway magnitude, sway frequency, postural transition dynamics	~8
Device interaction	Pickup gesture, texting micro-movements, pocket-to-hand transition	~10

4.3 Touch Features (Screen)

Feature Class	Examples	Count
Pressure dynamics	Mean pressure, pressure variability, pressure curve shape per tap	~8
Timing	Inter-tap interval, hold duration, swipe velocity profile, acceleration	~10
Spatial	Touch area, drift during hold, swipe curvature, target offset patterns	~7

4.4 Feature Vector Assembly

All features are z-score normalized against enrollment statistics. The complete identity vector I is the concatenation of all modality feature vectors, weighted by reliability:

> I = [w_c · F_cardiac, w_m · F_movement, w_t · F_touch, w_v · F_voice, w_i · F_impedance]
>
> where weights w reflect modality reliability (cardiac highest, barometric lowest)

5. Enrollment & Authentication Protocol

5.1 Enrollment

Duration: 60 seconds. User places finger on camera (PPG capture) while phone rests on surface (baseline accelerometer). App guides through:

- Seconds 0–40: Seated rest. PPG capture at 30fps. 40–60 cardiac cycles captured.
- Seconds 40–50: User speaks enrollment phrase ("I am [name], this is my voice"). Vocal spectral captured.
- Seconds 50–60: User picks up phone normally. Pickup gesture and transition dynamics captured.

Post-enrollment processing (on-device, <5 seconds):

- Extract feature vector I_enrolled from all captured modalities.
- Compute quality score per modality. Flag any modality below threshold (e.g., noisy PPG).
- Generate enrollment hash H(I_enrolled) for on-chain registration.
- Encrypt I_enrolled with device key. Store locally. Never transmit raw features.
- Generate Cardano wallet keypair. Encrypt private key with biometric gate.

> *The biometric feature vector NEVER leaves the device.*
>
> *Only the hash H(I) is registered on-chain.*
>
> *The private key is encrypted with the biometric — not derived from it.*
>
> *Biometric gates the key. Biometric does not become the key.*

5.2 Authentication (Unlock)

User touches phone. Within 2–3 seconds, passive sensors capture:

- Touch dynamics from the unlock gesture itself (pressure, timing, area).
- Accelerometer signature from pickup motion.
- If finger on camera: rapid PPG (5–10 beats, ~8 seconds for full cardiac auth).

Authentication levels:

Level	Modalities	Time	Confidence	Use

Quick	Touch + accelerometer	< 2 sec	$\theta = 0.80$	App unlock, low-value actions
Standard	Touch + accel + PPG (5 beats)	~8 sec	$\theta = 0.90$	Wallet access, transactions
High	Touch + accel + PPG (20+ beats) + voice	~30 sec	$\theta = 0.95$	Large transactions, identity verification
Forensic	All modalities, extended capture	~60 sec	$\theta = 0.98$	Legal identity, evidence submission

5.3 Continuous Authentication

While the phone is in use, accelerometer and touch dynamics are captured passively. A rolling window (30 seconds) computes similarity to enrollment. If similarity drops below $\theta_{continuous} = 0.75$ (indicating different person is using device), the session locks and requires standard re-authentication.

This means: if you hand your phone to someone else, UltraLife locks within 30 seconds. No explicit action required. The waveform shift is the lock.

5.4 Enrollment Evolution

The identity vector is not static. It updates slowly over time to accommodate aging, fitness changes, and other gradual shifts:

- After each successful high-confidence authentication ($\theta > 0.92$), the enrollment vector is updated: $I_{new} = 0.99 \cdot I_{old} + 0.01 \cdot I_{live}$
- This slow drift rate tracks genuine biological aging (gradual) while rejecting sudden shifts (someone else).
- Major enrollment updates (e.g., post-surgery, significant fitness change) require re-enrollment ceremony with higher scrutiny.

6. Cardano Integration — Aiken Validators

6.1 Identity Validator

The biometric identity maps to UltraLife's existing Aiken validator architecture. A new validator, identity.ak, handles biometric registration and verification:

```
Datum: { enrollment_hash: Hash<Blake2b256>, enrollment_time: POSIXTime,
      device_pubkey: PubKeyHash, confidence_history: List<Int>,
      status: IdentityStatus }

Redeemer: Authenticate { live_hash: Hash<Blake2b256>, confidence: Int,
                device_sig: Signature, timestamp: POSIXTime }

Validation: verify device_sig, check confidence >= threshold,
        check timestamp freshness, check enrollment is active
```

The critical insight: the raw biometric vector never appears on-chain. Only hashes and confidence scores. The validator confirms that a device holding the enrolled biometric has authenticated at a specified confidence level. Zero-knowledge proofs (Phase 2) will allow proving identity match without revealing even the hash.

6.2 Transaction Flow

A biometrically-authenticated UltraLife transaction:

- User initiates action (natural language: "send 50 ADA to [name]").
- Phone captures live biometric. Computes similarity to enrollment. If θ > 0.90, proceeds.
- Device signs transaction with private key (which was decrypted by biometric gate).
- Transaction includes: device signature + confidence level + timestamp.
- Identity validator checks: signature valid, confidence sufficient, timestamp fresh, enrollment active.
- Transaction executes. No password entered. No seed phrase exposed. The heartbeat authorized it.

6.3 Recovery

The hardest problem in biometric-gated keys: what if the device is destroyed?

Recovery Method	Security	Mechanism
Multi-device enrollment	High	Same biometric enrolled on multiple devices. Any device can sign. Losing one doesn’t lose identity.
Social recovery (Shamir)	High	Key fragments distributed to N trusted contacts. M-of-N required to reconstruct. Each fragment biometric-gated on holder’s device.
Re-enrollment ceremony	Medium	In-person identity verification + full biometric re-enrollment generates new key linked to same on-chain identity. Requires N-of-M social attestation.
Time-locked recovery	Medium	Pre-registered recovery key activates after T days of primary key inactivity. Allows migration without social contacts.

> *Seed phrases are eliminated entirely from the user experience.*
>
> *The user’s body is their credential. Social recovery replaces paper backup.*
>
> *This is the “invisible interface” philosophy applied to cryptographic identity.*

7. The Genotype-Waveform Convergence

This section maps the path from waveform identity to genetic identity equivalence.

7.1 What DNA Encodes vs. What Waveform Reads

Genetic Layer	DNA Encodes	Waveform Expression	Sensor Required
Ion channels	SCN5A, KCNQ1, KCNH2 — channel kinetics	Cardiac waveform morphology (QRS shape, QT interval)	PPG (phone) / Piezo (crystal)
Structural proteins	Collagen, elastin, keratin variants	Tissue impedance, bone resonance, skin conductance	Impedance spectroscopy (crystal)
Metabolic enzymes	CYP450 family, metabolic pathway variants	Thermal patterns, metabolic rate, respiratory quotient	Thermal + respiratory (crystal)
Muscle fiber composition	ACTN3, ACE — fast/slow twitch ratios	Movement dynamics, fatigue curves, gait efficiency	Accelerometer (phone)
Autonomic regulation	Adrenergic receptor variants	HRV patterns, stress response dynamics, recovery curves	PPG (phone) / Piezo (crystal)
Vocal tract geometry	Craniofacial development genes	Vocal resonance frequencies, formant structure	Microphone (phone)

7.2 Resolution Ladder

Phase	Resolution	Identity Equivalent	Health Equivalent
Phone (now)	Low-medium	Fingerprint-grade: unique, stable, verifiable	Fitness tracker: HR, HRV, activity level
Crystal v1	Medium-high	DNA-STR-grade: highly unique, multi-modal	Clinical screen: arrhythmia, stress, sleep quality
Crystal v2 + impedance	High	Beyond DNA-STR: includes phenotypic expression	Diagnostic: tissue composition, metabolic state
Crystal v3 + population data	Very high	Genotype inference: predict genetic variants from waveform	Genetic predisposition screening without DNA test

The convergence is gradual, not binary. Each hardware generation reads deeper into genetically-determined structure. Population-scale waveform-genome correlation studies (Phase 3–4) build the mapping function that connects waveform features to genetic variants.

> *DNA is the blueprint. Waveform is the building inspection.*
>
> *The building tells you what was actually built, how it’s being maintained, and how it’s performing right now. That’s more useful than the blueprint for every practical purpose except reproductive genetics.*

8. Forensic Evidence Framework

8.1 Evidence Classes

Level	Evidence	Strength	DNA Equivalent
Presence	Spectral signature within range of mesh node at time T	Strong. Time-locked. Biometrically certain.	DNA at scene (but with timestamp)
Proximity	Two signatures within coupling distance at time T	Very strong. Bilateral. Simultaneous.	DNA transfer between two parties
State	Signature shows sympathetic activation during event	Strong. Physiologically verifiable.	No DNA equivalent
Interaction	Coupling dynamics show approach / contact / retreat	Medium. Requires interpretation.	No DNA equivalent

8.2 Evidence Submission Protocol

- Victim or witness opens UltraLife app. Initiates evidence submission.
- Forensic-level authentication ($\theta = 0.98$, all modalities, 60 seconds).
- Device uploads encrypted waveform recording for specified time window.
- Recording is hashed and registered on Cardano with timestamp. Immutable.
- Decryption key held by submitter. Released to law enforcement via smart contract with judicial authorization (on-chain warrant).
- Suspect’s device recording obtainable via traditional warrant. Coupling events either corroborate or contradict.

> *Evidence ownership: the individual controls their recording.*
>
> *The mesh stores nothing. Personal devices store personal data.*
>
> *Forensic access requires consent (victim) or warrant (suspect).*
>
> *Cardano immutability prevents evidence tampering after submission.*

8.3 Chain of Custody

Traditional chain of custody requires documenting every person who handled physical evidence. Digital waveform evidence on Cardano has cryptographic chain of custody:

- Recording signed by device key at time of capture.

- Device key is biometric-gated (recording provably came from this person’s device).
- Submission hash registered on-chain at submission time.
- Any modification to the recording after submission breaks the hash.
- Cardano block timestamp provides independent time verification.

This is stronger than physical chain of custody because it’s mathematically verifiable rather than procedurally dependent.

9. Adversarial Model — Faraday & Spoofing

9.1 Threat Taxonomy

Attack	Difficulty	Detection Method	Residual Risk
Faraday shielding (block emissions)	Easy ($30 fabric)	Absence of any biological signal in area of physical presence. Thermal shadow mismatch.	Moderate — absence is detectable but not attributable
Replay attack (recorded waveform)	Medium	Liveness: no beat-to-beat HRV variation, no respiratory coupling, statistical regularity	Low — well-understood countermeasure
Waveform synthesis (modeled fake)	Hard	Cross-modal inconsistency: cardiac-movement coupling absent, touch dynamics missing	Medium — improves with attacker sophistication
Device compromise (extract enrolled template)	Hard	Template is encrypted, biometric-gated. Extraction requires physical device + biometric.	Low — equivalent to stealing hardware wallet + PIN
Multi-modal deepfake (all channels)	Very hard	Triangulation anomaly: radiation pattern inconsistent with real body. Thermal mismatch.	Low-medium — requires nation-state resources

9.2 Multi-Modal Defense Stack

The defense is not any single detection method. It is the cross-modal correlation that a real body produces naturally and that a spoofing system must simulate across every modality simultaneously:

- Cardiac-respiratory coupling: real hearts show respiratory sinus arrhythmia. Fakes typically don’t model this.
- Cardiac-movement coupling: exercise increases HR with specific temporal dynamics. Spoofing must model exercise physiology.
- Acoustic-electromagnetic match: real heartbeat produces correlated sound and EM field. Faraday blocks EM but not acoustic.
- Thermal-metabolic consistency: body temperature correlates with activity level and cardiac output. Suit disrupts this.
- Multi-node triangulation: real body radiates from volume. Surface transducers have wrong radiation pattern.

Each additional modality makes spoofing exponentially harder. Phone phase has 4–5 modalities. Crystal phase has 7+. An attacker must maintain consistency across all of them simultaneously.

9.3 Honest Assessment

> *Waveform identity is not unfoolable. No biometric is.*
>
> *It is harder to spoof than any existing single biometric,*
>
> *and the multi-modal architecture makes it harder than multi-factor authentication.*
>
> *The correct claim: “exponentially harder to spoof, not impossible.”*
>
> *The forensic claim: “strong corroborative evidence, not absolute proof.”*

10. Privacy & Consent Architecture

10.1 Core Principles

> *1. Your waveform data belongs to you. Period.*
>
> *2. Raw biometric features never leave your device.*
>
> *3. The mesh facilitates coupling but stores nothing.*
>
> *4. Forensic evidence requires your explicit consent or judicial warrant.*
>
> *5. You can delete your identity at any time. Deletion is permanent and verifiable.*

10.2 Data Sovereignty

Data	Stored Where	Accessible By	Deletion
Raw biometric features	Device only, encrypted	Device owner only (biometric gate)	Device reset deletes permanently
Enrollment hash	Cardano blockchain	Public (but hash reveals nothing about biometric)	On-chain revocation marks identity as inactive
Waveform recordings	Device only, encrypted	Owner. Law enforcement via warrant + smart contract.	Owner can delete at any time
Coupling events	Both devices, locally	Each party sees only their own record	Each party deletes independently
Confidence scores	On-chain (per transaction)	Public (confidence level, not biometric data)	Immutable once submitted

10.3 Consent Tiers

Tier	What It Means	Default
Identity only	Device authenticates you. No recording stored. No mesh interaction.	On (minimum for UltraLife)
Health monitoring	Device records your waveform for health insights. Stored locally.	User chooses at setup
Mesh presence	Your device participates in mesh coupling. Others detect your	Off by default

	presence.	
Forensic recording	Your device stores time-stamped waveform recordings for potential evidence.	Off by default
Coupling sharing	Coupling events shared with paired contacts (partner, family, team).	Off. Requires mutual opt-in.

Every tier is independently controllable. A user can authenticate with waveform (Tier 1) without ever enabling mesh presence or forensic recording. The privacy-maximalist configuration: Tier 1 only, no recordings, no mesh. It still works as a wallet and identity system.

11. Implementation Roadmap

Phase	Timeline	Deliverable	Identity Capability
Phone MVP	Month 1–3	iOS/Android app: PPG enrollment + touch/accel continuous auth + Cardano wallet	Fingerprint-equivalent. Seed phrase eliminated. 3–4 modalities.
Phone v2	Month 4–6	Forensic recording. Evidence validator on Cardano. Social recovery.	Evidence-grade with timestamps. Coupling detection via Bluetooth.
Crystal v1	Month 7–12	Resonance device: piezo cardiac + filterbank + basic impedance	DNA-STR-equivalent. 6–7 modalities. Health monitoring emerges.
Crystal v2	Month 13–18	Full impedance spectroscopy. Mesh networking. Material sensing.	Beyond DNA. Phenotypic expression. Forensic mesh capability.
Population study	Month 12–24	IRB-approved waveform-genome correlation study (1000+ subjects)	Build the mapping function f between waveform and genotype.
Crystal v3	Month 24–36	Genotype inference from waveform. Predictive health. Full convergence.	Waveform reading predicts genetic variants. DNA test without DNA.

11.1 Phone MVP Specification

The minimum viable product ships as an iOS/Android app with no hardware dependency:

- Enrollment: 60-second ceremony (PPG + voice + pickup gesture).
- Authentication: Quick (touch + accel, 2 sec), Standard (+ PPG, 8 sec), High (+ voice, 30 sec).
- Continuous auth: Passive accelerometer + touch monitoring. Auto-lock on identity shift.
- Cardano wallet: Full Cardano wallet functionality. Biometric-gated transaction signing.
- Social recovery: Shamir secret sharing across trusted contacts' devices.
- UI: Invisible. Natural language interface per UltraLife philosophy. No traditional wallet UI.

> *Phone MVP can ship independently of Resonance hardware timeline.*
>
> *It validates the identity architecture, builds the user base,*

> *and generates the population-level data needed for genotype convergence.*
>
> *When the crystal ships, enrolled users upgrade seamlessly.*

12. Honest Limitations

Limitation	Impact	Mitigation
PPG quality varies by skin tone	Melanin absorbs light differently. Darker skin = lower SNR in PPG.	Multi-wavelength camera (green + IR). Ensure enrollment quality check. Diverse training data.
Cold hands degrade PPG	Vasoconstriction reduces pulse amplitude.	Enrollment quality gate. Fallback to touch + accel auth when PPG quality drops.
Cardiac conditions affect waveform	Atrial fibrillation, pacemakers, arrhythmias change cardiac morphology unpredictably.	Enrollment flags irregular rhythm. Adaptive enrollment with wider tolerance bands. Secondary modalities carry more weight.
Movement artifacts	Walking, running corrupt PPG and accelerometer signals simultaneously.	Activity-state-aware authentication. Different models for rest, walking, running.
Population uniqueness unproven	Theoretical uniqueness is high. Empirical proof requires large-scale study.	EXP-004 is the first step. Population study in roadmap. Ship with conservative confidence thresholds.
Faraday spoofing is physically possible	Motivated attacker can block and potentially spoof waveform.	Multi-modal defense. Honest positioning as “exponentially harder” not “impossible.”
Legal admissibility untested	No court precedent for waveform forensic evidence.	Build evidence standard in parallel with technology. Expert testimony framework. Peer-reviewed validation studies.
Genetic inference is speculative	Waveform-to-genotype mapping requires population data that doesn’t exist yet.	Phase 3–4 goal, not Phase 1 claim. IRB study in roadmap. Honest about timeline.

> *This specification describes a system that can be built incrementally,*
>
> *validated at each stage, and deployed with honest confidence levels.*
>
> *The phone MVP is buildable now. The crystal enhances it.*
>
> *The genetic convergence is a research goal, not a launch promise.*
>
> *Every claim has a measurement plan. Every measurement has a kill criterion.*

Your body is your credential. Your heartbeat is your signature. Your waveform is your DNA.

UltraLife Protocol · resonance.systems · ultralife.io